

## VIVOTEK Product Security Advisory

**Advisory ID:** VVTK-SA-2018-003

**CVE ID:** CVE-2018-14768, CVE-2018-14771, CVE-2018-14770

**First Published:** August 24, 2018

**Last Update:** August 24, 2018

**Status:** Fixed

**Revision:** 1

### Overview:

Security researcher WeaponX of NSFOCUS Security Team and Ayushman Dutta discovered that some of CGI can be abused to command injection.

CVE-2018-14768, found by WeaponX of NSFOCUS Security Team, allows authenticated users to execute arbitrary commands on a vulnerable version via `update_lens.cgi`.

CVE-2018-14771, found by WeaponX of NSFOCUS Security Team, allows authenticated users to execute arbitrary commands on a vulnerable version via `eventsript.cgi`

CVE-2018-14770, found by Ayushman Dutta, allows authenticated users to execute arbitrary commands on a vulnerable version via ONVIF interface (`/onvif/device_service`).

### Affect Products:

All Network Camera Series using firmware prior to XXXXXX-VVTK-0X06a.

### Workarounds:

None.

### Solution:

Please upgrade firmware to XXXXXX-VVTK-0X06a or above.

#### Alert:

Due to CSRF protection solution, after upgraded you camera firmware, please also upgrade your Shepherd to version 3.0 or above to make all operations function normally.

### Revision History:

Revision 1 / August 24, 2018 / Initial release